Network Management Architecture Guidelines

Commonwealth of Massachusetts Committee on Information Technology Version 2.0

July 1998*Presented by the Strategic Planning Bureau of the Information Technology Division*

Table of Contents:

Network Elements and Management Responsibilities

Management Recommendations

Conclusion

Executive Summary

Opportunity

The Commonwealth and its agencies have committed to building a common enterprise network in order to reduce the Commonwealth's expenditure on telecommunications and to promote connectivity and interoperability among various state agencies. As the Commonwealth plans to put this infrastructure in place, it must recognize that the cost of building such an infrastructure includes the cost of making this infrastructure manageable. An enterprise network that cannot be managed will not be capable of providing reliable, cost effective service to state agencies. A consistent, carefully architected and implemented management solution will ensure that network operations staff are able to diagnose and troubleshoot failure; to proactively administer the network to avoid downtime; to maintain accurate records of network usage and services levels; and to ensure that the network provides the production-quality, industrial-strength platform required for the business of state agencies.

Integrating Diverse Systems

The Commonwealth is currently in the process of establishing networking and computing standards aimed at evolving the State's computing and networking environments toward greater connectivity and interoperability. The Commonwealth of Massachusetts Committee on Information Technology has drafted standards for desktop computers, for local area networks, and for network architecture. This document is the standard for network management.

Management Challenges

There are several challenges that the Commonwealth must meet in order to create an effective network and systems management environment for both the MAGNet enterprise backbone and agency networks. The most significant will be evolving from a diverse mixture of proprietary point product element management systems (EMSs), aimed at managing only a single component type of the network or systems environment, to a system that is capable of integrating the management for many network components and systems. For example, different agencies may use different modems to provide WAN connections, and each modem vendor provides an EMS (or application) that manages only their own modems. Historically, vendors of PBXs, terminal servers, minicomputers, and personal computers have all taken the same approach to managing their products. A better approach is to manage all of these computing and communications elements via an integrated solution using common platforms wherever possible.

Another important challenge for the Commonwealth will be to define and divide management roles and responsibilities between agency network administrators and the centralized staff. While each group will have primary responsibility for managing a different part of the network, pieces of the network may fall into the domain of shared responsibility.

Finally, while many of the elements in agency networks use proprietary messaging techniques between the management application/platform (manager) and the managed device (agent), a new management solution must embrace open, industry standard management protocols (for manager/agent messaging) and application programming interfaces (APIs).

Five Disciplines of Network Management

Network management should be thought of as information systems for networks. It allows management to examine the way in that an important capital resource is being used, and provides the necessary information for adjusting the operation of that resource so it more closely meets the needs of the organization. It involves the usage of information technology to measure and manage the effectiveness of the organization's networks. The overall goal of network management is to maximize network availability, performance, and benefits to network users. This

is accomplished through five basic management activities, each of that must be provided in an effective enterprise management system:

Fault Management is the discipline of detecting, diagnosing, bypassing, repairing, and reporting on network equipment and service failures. Fault management tells the manager what the network is doing.

Configuration and Name Management is concerned with maintaining an accurate inventory of hardware, software, and circuits in use throughout the enterprise, and provides the ability to change that inventory in a reliable and efficient manner in response to changing service requirements. Configuration and name management ensures the consistency and validity of operating parameters, addressing tables, software images, and hardware configurations. Configuration management tells the manager where everything is in the network.

Performance Management is concerned with tracking and planning for the best utilization of network and computing resources and ensuring that the required resources are available to meet user service level expectations. Performance management tells the manager how the network is doing.

Security Management controls access to both the network and the network management systems. It protects the network and its management systems from unauthorized access or modification. Security management tells the manager who is using the network.

Accounting Management measures network usage and computes charges for that usage. It tells the manager when the network is being used and the cost of the resources consumed.

Network Architecture

The network architecture for the Commonwealth of Massachusetts is depicted in Figure 1. It consists of a core backbone network, called MAGNet, and attached agency networks. MAGNet is composed of an ATM Metropolitan Area Network (MAN) interconnected with a wide area network of T1 and frame relay links. Over a period of time the T1 and frame relay links are being replaced by ATM connections. Although the Commonwealth's enterprise network has been designed to accommodate multiple protocols, it is the goal of the architecture to converge the enterprise on one open standard.

Figure 1: Commonwealth of Massachusetts Network Architecture

The major target protocol standards for this architecture are TCP/IP and the OSPF routing protocols. Convergence on these standards is an important step toward interoperability between systems across every organization in the Commonwealth.

Division of Management Responsibilities

As indicated in Figure 1, agencies interface to MAGNET at the "Service Access Point" (SAP). The SAPs indicate the line of demarcation between components of the network managed by ITD CSB and the components managed by individual agencies. For convenience, components on the MAGNET side of the SAP are identified as "Core Hubs" (CH), and those components on the agency side of the SAP are identified as "Group Hubs" (GH).

The management of the logical network is shared between individual state agencies and the Information Technology Division's Communications Service Bureau (ITD CSB). Agencies have the responsibility of managing the logical network from the end-systems to and including the GH, while ITD CSB manages the logical network from and including the CH into the wide-area. The links between the GH and the CH may fall into a shared management domain, but is usually the responsibility of the agency. Large executive agencies with internetworking expertise may negotiate with ITD CSB to manage this link, or at their discretion, request that this link be managed for them. It is, however, in the best interest of individual agencies to have ITD CSB manage the GH-CH links wherever possible. The GH-CH connections are stable and will not change as frequently as the GH-ES links. Agencies operating with limited resources probably do not have the personnel or the training dollars to take on this responsibility.

Figure 1 illustrates the separation in logical network responsibilities. Components to the right of the SAP are normally managed by ITD CSB, and those to the left of the SAP are normally managed by the agencies. Agencies may negotiate with ITD CSB to manage the GHs.

ITD CSB establishes the guidelines for the protocols that may traverse between CHs in the MAGNet backbones while individual agencies have the freedom to choose the logical networks they will support and use. For those protocols which will be used on an enterprise scale, ITD CSB has the responsibility for naming and address policy/distribution. ITD CSB has acquired two Class-B IP address for the Commonwealth and all of its agencies. ITD CSB has the responsibility for providing blocks of addresses to individual state agencies, which in turn have the responsibility for assigning addresses to particular network devices.

Management Architecture

The Commonwealth of Massachusetts and its agencies are facing many of the same challenges that face modern business organizations. The requirement to provide increasingly higher levels of service with fewer resources is a common theme among large enterprises operating in an intensely competitive global marketplace. Network support and operations organizations are under the same pressures: to improve efficiency and efficacy in a time of scarce resources. This trend is causing most large enterprises to seek highly intelligent automated network management solutions. The strategy of substituting network management tools for network management staff promises to be an effective means to meet the requirement "to do more with less."

Management Approach

A Legacy of Heterogeneous Systems and Networks

Historically, the Commonwealth has provided to state agencies a wide degree of freedom in selecting and deploying computer systems and networks. This decentralized approach to procurement has resulted in a heterogeneous computing and networking environment. As illustrated in Figure 2, many agency systems and networks are managed via proprietary management platforms and applications created by the vendor who supplied the system. However, managing the entire Commonwealth's systems and networking environment, or even a single agency's network and systems by means of many proprietary management applications is an arduous task. Therefore, a unified approach to managing the majority of the critical networking and computing assets must be undertaken.

Figure 2: Multiple Separate Proprietary Managers

The Evolution of Management Approaches

The approaches to integrated management of a multivendor computing and communications environment have been evolving in the marketplace over the

past several years. Figure 4 illustrates the first integration architecture, known as the Manager of Managers or MOM architecture. Structured hierarchically, it provides an integrated view of the network by interfacing a number of proprietary element management systems into a single integrated management system. The other architectural approach for achieving integrated network management is known as the Open Management Platform or OMP architecture. The OMP approach (see Figure 5) is a more distributed approach than the MOM approach, since it links integrated management systems directly to managed elements using open protocols like the Simple Network Management Protocol (SNMP) and allows for distribution of the management functionality among the different managers. The OMP also features open application programming interfaces (APIs) that allow many vendors to supply software components (e.g., applications, objects, or data definitions) that run on top of the platform. The next two sections examine the MOM and OMP approaches more closely.

Manager of Managers (MOM)

The MOM products (e.g. mainframe-based NetView) have primarily concentrated on integrating the management of the installed base of network elements and centralized computers that are not equipped with open management protocols. Such products are designed to manage legacy network devices. The major banks, airlines, retail chains, and insurance companies with large, mature, mission-critical networks have not benefited much to date from developments in open management such as SNMP. They have a wide variety of management systems, and they are willing generally to pay for improved management functionality of a MOM that can bring them all together into a single management system.

MOMs integrate information from existing device- and vendor-specific management systems using a variety of techniques, most of that involve some form of emulation. To a standards advocate, the methods used by MOMs to interface with installed vendor specific Element Management Systems (EMSs) are downright kludgey and the whole approach jerry-rigged. Typically, a MOM will connect to the EMS printer port that will be set up to print an alarm log to that port. Thus, the MOM gets a set of print characters that it is able to parse into a set of alarm messages. On the control side, the MOM connects to a console port or perhaps uses a remote log-on protocol to provide a terminal session with the EMS. Most MOM products have scripting facilities that can be used to set up the proper sequence of EMS text commands to accomplish different tasks, such as showing the detailed status of a particular device.

Because of the nature of their interfaces, MOMs are limited in the functions that they can implement. You can only do so much with alarms. For example, it is very difficult to do performance analysis with this source of information. Most MOM products concentrate on filtering and consolidating alarm information. Most

importantly, they have focused on automating responses to alarm conditions, since this is the kind of function around which a business case for improved management can be made. Unfortunately, even where management automation is fairly sophisticated, management through the MOM architecture often relegates the manager to reactive management. Managers respond to alarms, fix a problem, and move on to the next most critical network error since they lack the necessary management tools to address problems in a proactive manner.

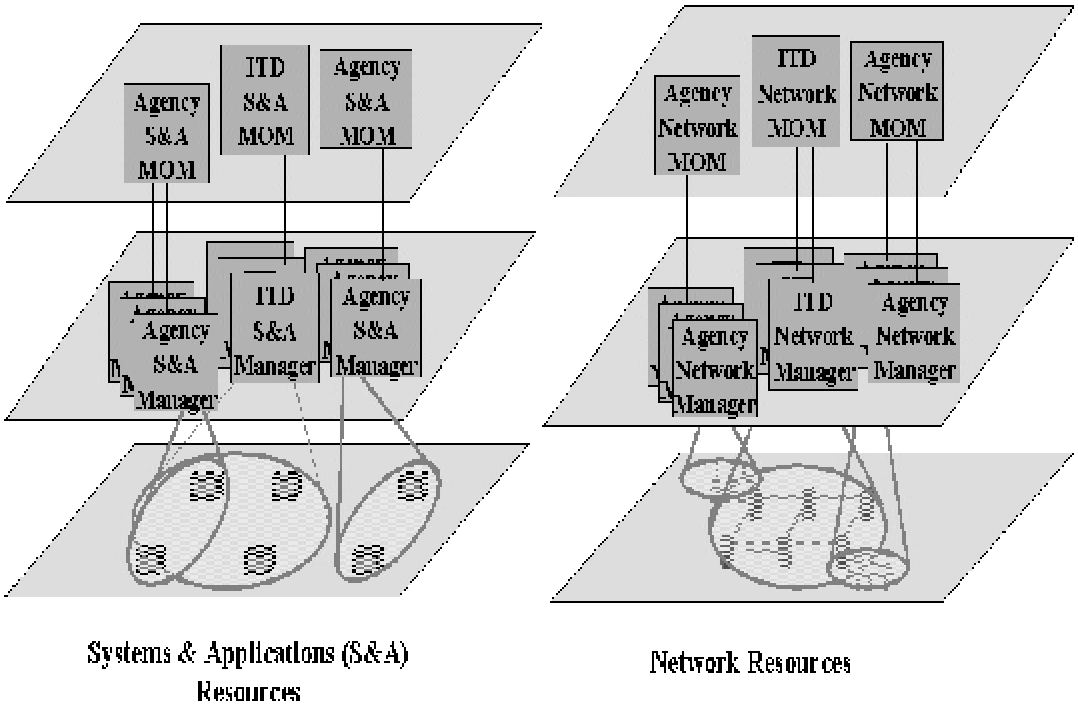

Figure 3: The Manager of Managers (MOM) Approach

Open Management Platform (OMP)

The open management platforms have targeted a completely different market and use a completely different strategy for integration. Rather than deal with the mess of the installed base of legacy management systems, the OMP vendors have gone after the rapidly growing market for standards based LANs, LAN interconnect, and client-server computing. These new computing systems were designed explicitly for multivendor environments.

Figure 4 illustrates the OMP approach. Note that, although they look the same architecturally, the approach to achieving open management has differed in the networking community and the systems & applications community.

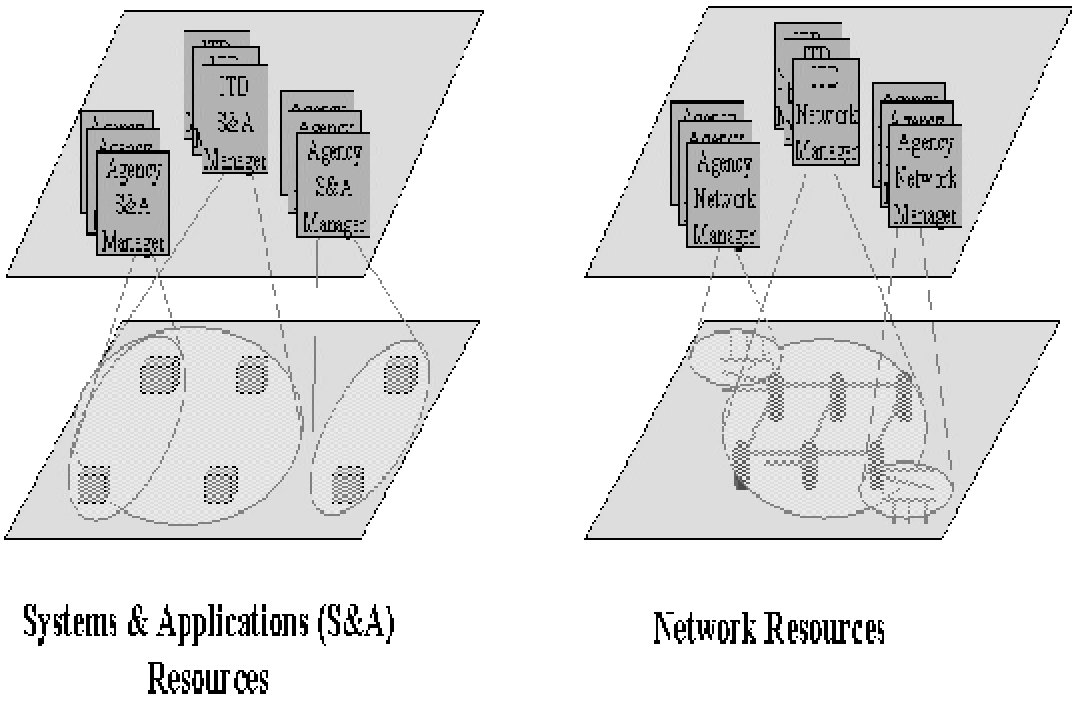

Figure 4: The Open Management Platform (OMP) Approach

OMP Approach to Integrated Network Management

The networking community took the standards approach by first standardizing on management protocols, the structure of management information, and a subset of the management information. Then they developed products based on those standards. These products for network management have matured over the last several years. The internet community has standardized on the Simple Network Management Protocol (SNMP) and associated SMI and definitions of management information. Open management is now a widely held principle in the internetworking market. The telecommunications community has standardized on the Common Management Information Service/Protocol (CMIS/CMIP) and the associated OSI management SMI and management definitions. Carrier telecommunications networks are now being converted to use Telecommunications Management Network (TMN) principles and standards.

Since it has exploded into the mainstream, the private, multiprotocol internet has a large portion of its elements relatively new and SNMP-ready. The big growth environment in most enterprises today is the multiprotocol internet that is filling up with client-server systems. Although older mission-critical transaction processing systems are still there, they are not usually growing and the newer client-server systems have exceeded the previous generation in terms of both the number of elements to manage and system complexity.

Network management OMPs today primarily use SNMP to retrieve management information directly from the network resources. The major network management OMPs are based on a UNIX-oriented or Windows NT-oriented manager-agent architecture. The main feature of network management OMPs is their open application programming interfaces (APIs) that allow other vendors to integrate software modules or complex management data definitions (known as management information bases or MIBs) onto the OMP server. The OMP approach has generated a healthy independent software vendor market that created a variety of network management applications and tools that run on the leading platforms. In addition, the major network systems vendors provide platform-based management tools for their products (e.g. Cisco Works or BayNetworks Optivity), thus eliminating the need for a separate proprietary EMS workstation. The ability to add many different kinds of software modules to the basic platform give network management OMPs a wide range of potential functionality that the closed MOMs will never be able to duplicate.

Because they have protocol access to network elements, network management OMPs can implement a wider range of functionality than MOMs can. Today's network management OMPs provide much more than alarm and status monitoring. They commonly provide automated discovery of network configuration information, performance monitoring, and protocol analysis. Most network management OMPs have not concentrated heavily on providing automated responses to faults, however, they provide basic filtering and consolidation of alarm information. Network management OMP vendors have concentrated instead on automating the discovery of configuration and inventory information.

The benefits of an OMP in the network management domain have been limited. The current network management platforms provide limited functionality in terms of auto-discovery of managed devices, browsing of MIBs for individual devices, and event management. However, they do not offer a vendor independent view of managed network elements, or an end-to-end view of network management. Device vendors have extended the MIBs required to manage their devices and provided vendor dependent applications to run on the platforms to manage their specific products. As a consequence little homogenization has occurred at the operator interface level. Operators must still deal with different proprietary applications and interfaces that are specific to vendor products, e.g., Cisco's CiscoWorks, or Bay Network's Optivity.

OMP Approach to Integrated Systems & Applications Management

As stated previously, the systems and applications community has been taking a slightly different approach to creating an OMP solution. The standards developed within the network management community have not been accepted within the systems and applications community, primarily because: the requirements differ, the constraints imposed on network management tools do not apply, e.g., the

assumption of dumb managed elements, and new object oriented standards for application development and interoperability have been developed. For example,

> Systems and applications managers have, to greater degree than network management, requirements to create and frequently change 100's or even 1000's of user accounts, distribute software and updates to 1000's of computers, synchronize computer workloads, and perform scheduled backups of 1000's of computers.
> Responsibilities for managing systems and applications is widely distributed, while network management can often be centralized because the network becomes a corporate resource. Thus the tools needed to partition management responsibilities and enforce management policies need to be much more distributed.
> Distributed object-oriented architectures have emerged, e.g., the Common Object Request Broker Architecture (CORBA) as the accepted paradigm for integration. In addition, due to market dominance, Microsoft's Distributed Common Object Model (DCOM) is becoming a defacto standard in the desktop management area.

In the desktop market, where network operating systems (NOSs) by Microsoft and Novell dominate, their respective network management systems also dominate. These product's capabilities include print, file services and management, user administration, security, automated asset inventory, and software distribution for MS Windows 3.x, 95, NT, IBM OS/2, and Macintosh OS desktops.

In the UNIX market, where individual vendors offer management of their own products, the current leading vendors of integrated management of multi-vendor UNIX systems are IBM/Tivoli and CA Unicenter. These product's capabilities include print, file services and management, user administration, security, automated asset inventory, workload management, and software distribution. In addition, they provide customer help desk solutions for trouble ticketing and service management, either themselves or via third party integrated solutions.

The emerging market is for systems and applications OMPs that can manage multivendor UNIX client-server and desktop environments. Such environments contain SUN, HP, DEC, IBM UNIX servers and workstations, and personal computers running Microsoft Windows 3.x, 95, NT, IBM OS/2, and MAC OS. A number of vendor proprietary solutions are vying for dominance in this area, with the two main contenders being IBM/Tivoli (TME 10), Computer Associates (CA Unicenter). The strength of both of these solutions is that they provide a framework upon which other vendors can provide management applications.

The main feature of systems and applications management OMPs is their open application programming interfaces (APIs) that allow other vendors to integrate software modules or complex management data definitions onto the OMP

servers. The OMP approach has generated a healthy independent software vendor market that is creating a variety of systems and applications management applications and tools that run on the leading platforms. In addition, the major systems and applications management framework vendors provide platform-based management tools for their products. The ability to add many different kinds of software modules to the basic platform give systems and applications management OMPs a wide range of potential functionality that the closed MOMs will never be able to duplicate.

The benefits of an OMP in the systems and applications management domain promise to exceed the benefits realized in the network management domain. An attempt at homogenization is occurring at the operator interface level. The framework vendors attempt to offer a consistent interface across multiple management applications - including those applications provided by third parties - and attempt to integrate those applications at the database level. Also, the individual management applications are able to manage resources from multiple vendors by mapping their differing management implementations into a common information model. Even though the common information model is currently non-standard, the advantages realized by having even a proprietary common information model far outweigh the disadvantages. As the systems and applications management area matures standards are being developed that will allow some elements of the proprietary solutions to disappear, e.g., the Common Information Model (CIM) being developed by the Desktop Management Task Force (DMTF).

Integrated Systems, Applications, and Network Management

As seen in Figures 3 & 4, the MOM and OMP approach can be applied separately to network management and to systems & applications management. However, an integrated approach that combines systems, applications, and network management is desired for end-to-end management of services expected by the users. The features of such a system include:

Single console for mainframe, mini and LAN-based systems.
Single console interface across multiple operating systems.
Single discovery and polling engine.
Single event-correlation engine for all events regardless of communications format (SNMP or vendor specific).
Single calendar for job control, software distribution, and security and policy enforcement.
Single security-access authorization for all managed systems and processes.
Sharing of data between applications (the helpdesk application has access to asset data, for example).

Again, either a MOM or OMP approach can be applied to this next level of integration.

Figure 5 illustrates a MOM approach to integrated systems, applications, and network management. This would introduce an additional level in the manager hierarchy with a separate manager for ITD and each agency. Again, the difficulties discussed previously concerning MOM architectures also apply here.

Figure 6 illustrates the OMP direction the community is seeking to take in developing an integrated and distributed systems, applications, and network management solution. The approach would enable each agency to manage all of its systems, applications, and network resources from one console. It is distributed in that the console may be accessed via any of the distributed platforms, subject to security policy constraints. Management access to resources would be constrained only by policy, and not by technology. The management would be flexible enough to accommodate changes in the resources accessed, the time at which they may be accessed, and who may access them. ITD and each agency would be able to manage their own systems, applications and network resources, and coordinate with each other the overall resource management, based on policy decisions.

Vendors in the systems and applications management community are spearheading the direction toward integration, illustrated in Figure 6. The approach the community is taking to achieve this integration is a continuation of the systems management OMP approach, i.e., extend their object-oriented frameworks to include network management capabilities. The same vendors who are dominant in the systems and applications area are also dominant in this area (IBM/Tivoli, CA/Unicenter). As expected, the standards emerging within the systems and applications management community are those that are beginning to dominate the systems and applications management area. The most important standards development is the emergence of the Common Object Request Broker Architecture (CORBA) as a method paradigm for integration, using RPC mechanisms for communication among management modules.

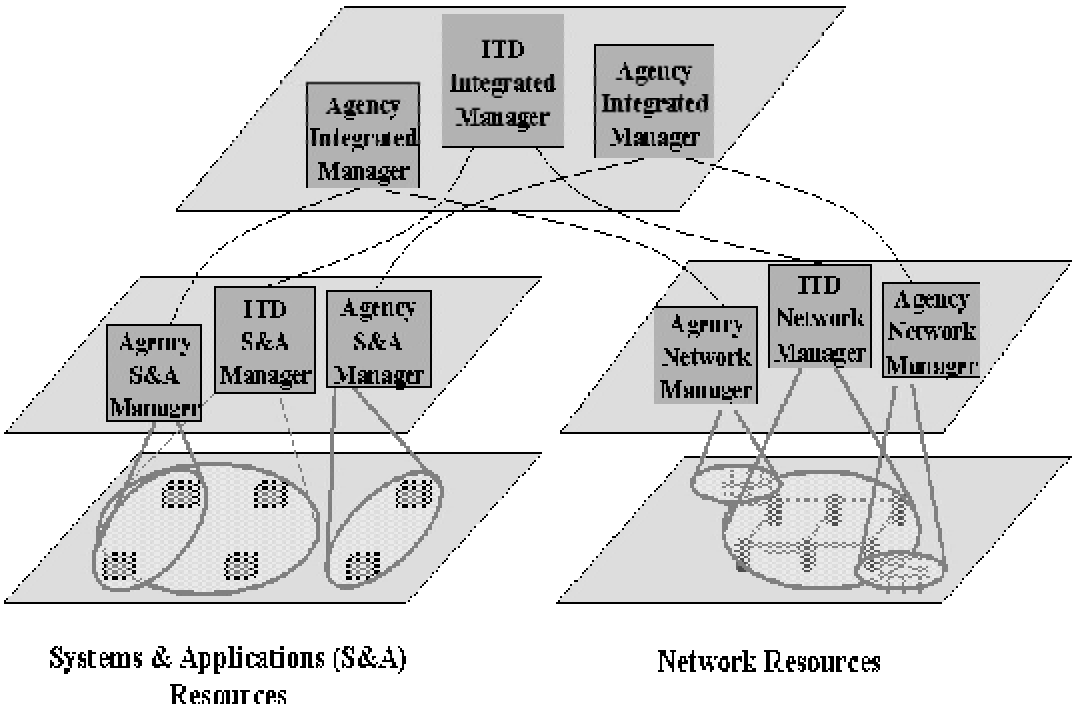

Figure 5: The Integrated MOM Approach for Systems, Applications, and Network Management

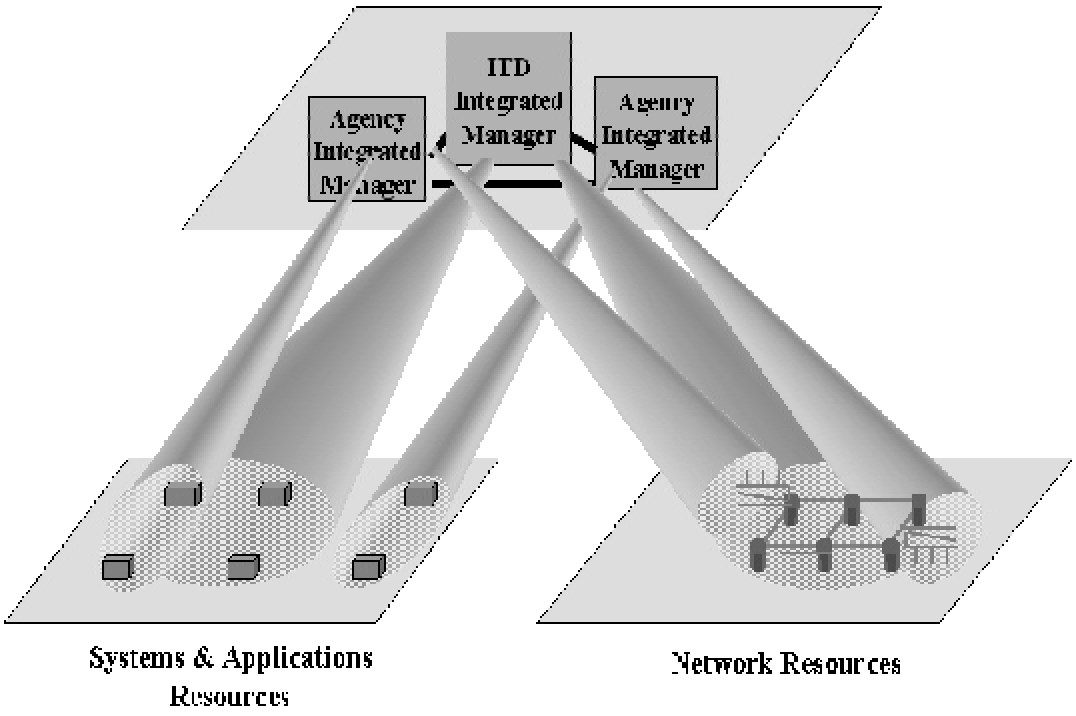

Figure 6: The Integrated OMP Approach for Systems, Applications, and Network Management

Figure 7 illustrates the current reality of integrated management of systems, applications and network resources. The systems and applications management vendors have extended their capabilities, using a MOM approach, to integrate leading network management vendor open management platforms into their architecture. The current level of integration is currently limited to event management and correlation, and providing access to the network manger console. However this situation is rapidly changing as vendors provide integration at the topology mapping and database level.

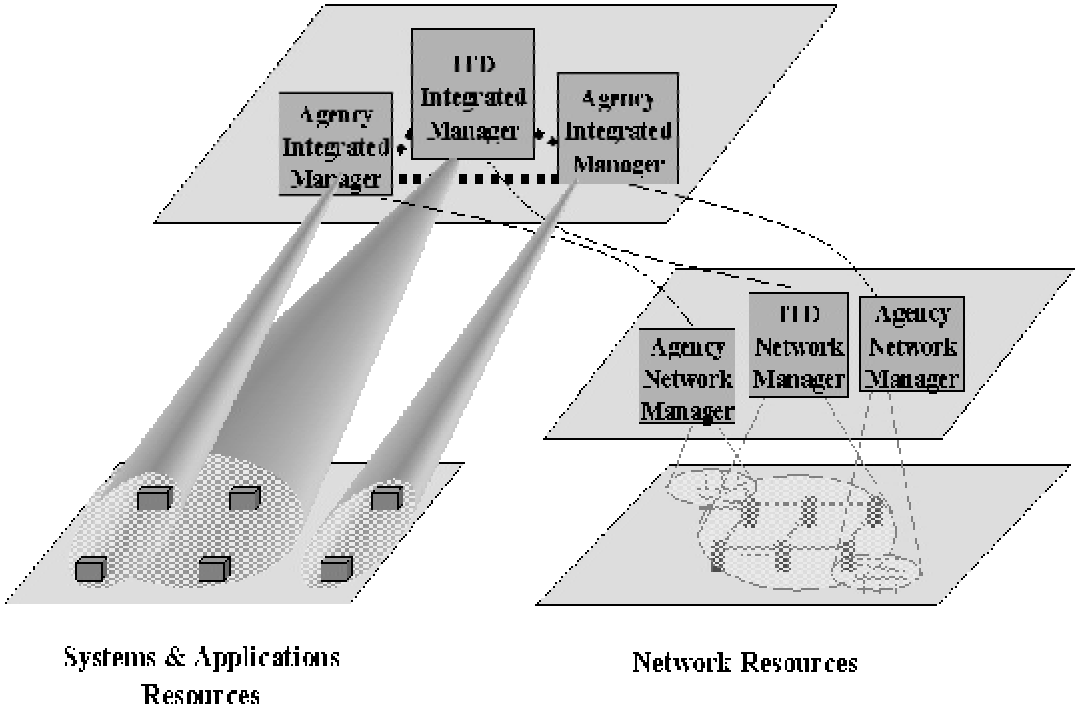

Figure 7: The Modified OMP Approach for Systems, Applications, and Network Management

The next section provides an overview of leading open management platforms.

Overview of Leading Network OMPs

Network management OMPs have matured over the last few years with the leading IP OMP vendors being HP, IBM, Cabletron, and SUN. Although mature, these products are constantly being updated. The product descriptions below only represent a snapshot of the current state of these products as of the time that this document is being written. The current status and capabilities of these products should be reviewed when making a purchase decision.

HP OpenView

HP's OpenView, currently the leading network OMP vendor, runs on the Sun workstation in addition to HP's own UNIX workstation. This allows vendors with applications running on Sun workstations to easily support the Sun version of OpenView and not have to go through the effort of porting their programs to HP's hardware and software. In addition, Openview is supported on the MS Windows NT platform. OpenView supports a distributed architecture with hierarchical or peer relationships among management workstations. It also supports intelligent agents for distributed polling and event forwarding.

HP has also been successful with the DOS/Windows versions of OpenView. This is a low-end product that is not distributed and that supports a limited set of features, but it is very popular with a variety of vendors as the basis for a low-end entry-level management product.

HP's OpenView Network Node Manager is the network management leader with third-party vendors. OpenView ships with more than 150 MIB definitions from vendors other than HP. Every major element manager ships a version of its software that runs on Network Node Manager, and this wide support currently makes it the favored network management platform.

HP's support for relational databases from Oracle and Ingres open the network management database to query with powerful RDBMS tools.

The strength of the OpenView product, both in terms of its market share and its technical foundation make it an attractive enterprise management platform. The capabilities of the product have encouraged a large number of independent software vendors to create applications for OpenView. In addition, ITD has chosen HP Openview for management of MAGNet. For these reasons, OpenView should be considered a candidate OMP for all State Agencies that have to manage SNMP compatible devices.

IBM/Tivoli TME/Netview

IBM/Tivoli TME/NetView runs on IBM' UNIX workstation (AIX) and on Windows NT. Originally, TME/Netview was based on the HP OpenView software licensed from HP but quickly diverged from HP's version of the product while maintaining compatibility with the original APIs. TME/NetView supports a distributed architecture with hierarchical or peer relationships among management workstations. It also supports intelligent agents for distributed polling and event forwarding.

IBM/Tivoli TME/Netview is currently in the process of being more tightly integrated with the IBM/Tivoli management framework. Thus it is a key component in the OMP for IBM/Tivoli's integrated systems, applications, and network management solution.

Given its growing strength in the management marketplace, IBM/Tivoli TME/NetView should also be considered a candidate for the State's open network management platform.

Cabletron Spectrum

The Cabletron SPECTRUM Enterprise Manager in many ways surpasses the capability of the HP OpenView Network Node Manager. It's object oriented architecture is especially applicable to fault isolation and diagnosis. SPECTRUM Enterprise Manager supports a distributed architecture with hierarchical or peer relationships among management workstations. It also supports intelligent agents for distributed polling and event forwarding. SPECTRUM is supported on SUN UNIX platforms and Microsoft's NT.

Given its growing strength in the management marketplace, Cabletron Spectrum should also be considered a candidate for the State's open network management platform.

SunNet Manager

The early leader in open management platforms was Sun Microsystems with its SunNet Manager platform. Sun had a huge advantage over other platform providers because the majority of management applications and stand-alone element managers in the industry had been implemented on Sun workstations and SunOS. Although everyone would like to believe that applications written to UNIX are portable, the fact of the matter is that it is still a great deal of work to move an application to another hardware and software platform, even if that other platform also runs UNIX. Since many vendors already had their software running on Sun's hardware and operating system, it was quite easy for them to do some integration with SunNet Manager, and they did. Because Sun could point to so many applications that could run with SunNet Manager, it gained a large following. Many users liked it because they already owned Sun workstations, and because they had bought some kind of management package that ran in this environment. Today, however, Sun's lead in this market has diminished. Sun has failed to add significant new functionality to SunNet Manager and does not appear to be investing in the product at the same level as other platform vendors.

Given the wide range of applications written for this platform and its role in core hub management, SunNet Manager should be considered as a candidate for the State's open management platform.

Overview of Leading Systems and Applications OMPs

The Systems and Applications management area is immature and volatile at this time with numerous point product solutions that address specific components of

systems and applications management, e.g., backup, software distribution, system monitoring, etc., and frameworks that seek to provide an integrated solution. Product offerings are updated on a 3 - 12 month schedule and competition is fierce between the current leading vendors (Computer Associates Unicenter, IBM/Tivoli TME10, HP IT/ServiceManager). In addition NOS vendors such as Novell and Microsoft provide solutions for their specific NOS environment. Consequently, The product descriptions below only represent a snapshot of the current state of these products as of the time that this document is being written. The current status and capabilities of these products should be reviewed when making a purchase decision. In addition, existing and new point product solutions not discussed here should be considered at the time of making a purchasing decision.

CA Unicenter TNG

CA Unicenter TNG is aimed at large enterprise network with hundreds, if not thousands, of users, and claims to support a range of operating systems and hardware platforms. Core-management options are provided for, including basics like hardware and software inventory, software distribution and remote control of servers and workstations. Integrating other management tools into the architectures, such as SNMP consoles and help-desk products as well as custom-made extensions, sold by independent third parties or developed in house, by end users can extend core management functionality.

CA has built up Unicenter TNG by acquisition of companies and their products to cover gaps in their functionality. This has resulted in inconsistencies in integration, e.g., some modules still retain much of the user interface developed for the original package. Not that any of this detracts from the functionality on offer, but it makes for confusion when you have to navigate your way around the package.

CA uses a proprietary object-oriented architecture, which calls for the use of distributed agents, each of which is specific to a set of management services. SNMP and proprietary protocols are used between managers and agents. Information gathered from these agents is stored in a central SQL Server database called the TNG Object Repository. You can view, query and report on this using what CA calls the WorldView component, with the collected data represented in 2D or 3D maps on one or more distributed management consoles. The same data can be used by separate Enterprise Management components, providing the core services of security, calendar and event management. These can be called directly from the WorldView interface or used by optional plug-in management modules, available from CA or an extensive list of partners and third parties. A published set of APIs and a software-development kit are available to enable in-house applications to be integrated into Unicenter.

You can set system and application-specific thresholds at the agent level, and messages and traps can be forwarded onto other administrators, if required. A separate Event Management Console is also included. This can handle alerts from the various TNG agents and more general SNMP traps and NT event log entries. You can set up rules-based filters at various levels to consolidate events from multiple sources and trigger automated responses where appropriate, both locally and on other remote servers on the network.

IBM/Tivoli TME 10

IBM/Tivoli is aimed at large enterprise network with hundreds, if not thousands, of users, and supports a range of operating systems and hardware platforms. Core-management options provided include basics like hardware and software inventory, software distribution and remote control of servers and workstations. TME 10 can be extended by integrating other management tools into the architectures, such as SNMP consoles and help-desk products as well as custom-made extensions, sold by independent third parties or developed in house, by end users.

Unlike most network-management products, TME 10 doesn't rely on the SNMP protocol as the transport for its management information. Taking a standards based approach to systems management that derives from the applications standards area, Tivoli's TME 10 provides a CORBA-compliant distributed object model, based on software known as the TME 10 Framework, and installed onto every node you want to manage on the network. This framework underpins the package, offering a set of common services available for use by all the Tivoli management tools and applications which can be used (and extended) by others available from partner companies and third-party developers. The framework integrates with software modules from third parties, as well as those of its own design, and works with a wide range of host platforms.

The basic facilities in the TME Framework include a DHCP service, security and task libraries, and a scheduling service. On top of these a number of management services can be added to support specific options, such as software distribution, user administration, network inventory and event management. As such, the TME 10 Framework provides a runtime environment for management applications that's independent of the host operating system. That makes for a consistent user interface, with no need for different versions of each application and no need to treat each type of platform differently when deploying the various tools on offer.

Frameworks for a number of different platforms are available, including 16-bit and 32-bit Windows, and 17 implementations of Unix, with OS/2, Novell IntranetWare, and (soon) S/390 mainframes and AS/400 minis. The administrative console--the TME 10 desktop--is built into most implementations of the Framework, providing a command-line interface and a GUI front end to

manage what Tivoli refers to as resources, policies and policy regions. These represent resources corresponding to the systems, devices, users and services on the network. Policies are the rules and conventions that govern the management of those resources, while a policy region groups together particular resources and the policies that govern them. It's possible to group application-specific information in the form of a profile and distribute it across the network to change the way particular resources are configured or monitored.

Because it's all rules-based, you don't need specialist knowledge to add new members of staff or change details when moving users from one location to another. The tasks involved can be delegated to help-desk operators or local administrators, rather than involving more expensive technical support staff every time. You can also integrate the procedure into a third-party application, like a help desk, so the operators don't have to see or be trained to use the TME 10 desktop.

The Tivoli Enterprise Console, or TEC, employs a system of distributed event adapters and event servers to intelligently manage events on the network. The event adapters are built into all the distributed monitoring collections, and specific adapters interface other applications, such as HP OpenView and IBM NetView/6000. These ship with a basic set of consolidation rules to handle common event situations, while extra rules can be written directly in a Prolog-like language or indirectly using a separate graphical rule editor. You can configure the software to handle events automatically, only passing on alerts to the console when it can't resolve the situation, then it shows you the status of each event, its history and any action that's been taken to resolve it.

HP Openview

HP initially entered the systems and applications management area with a suite of products based on its Openview platform. HP then paid little attention to the area and let CA and Tivoli gain the lead. Recently, however, HP has re-entered the competition with a service management orientation and an update of their loosely coupled set of systems and applications management products.

HP is aimed at large enterprise network with hundreds, if not thousands, of users, and supports a range of operating systems and hardware platforms. Core-management options provided include basics like hardware and software inventory, software distribution and remote control of servers and workstations. The HP solution consists of a loosely coupled suite of management applications that are integrated via the HP Openview GUI interface. The solution can be extended by integrating other third party management tools into the HPOV GUI. Although currently not an integrated framework, HP plans on evolving HP Openview into an integrated framework over the next few years.

The HP solution currently consists of:

IT/Administration - allows individual system administration tasks such as software distribution and the administration of user accounts across different platforms. IT/Administration provides a view of all managed systems: hardware inventory, installed software and the individual configuration of each system. Also included are flexible query capabilities, a change detection service, and role-based security.

HP OpenView IT/Operations - a distributed client/server software solution in which the server is a Central Management Console and the clients are Intelligent Agents. Intelligent agents can also be pre-configured to solve problems immediately without interacting with the central management console. IT/Operations provides access to the status of mission-critical systems, network infrastructures (including intranets), and business-critical applications such as Oracle databases, SAP R/3, Microsoft and Netscape internet servers, and Baan IV. Network and system performance data, enterprise-wide storage and backup information, hardware and software inventories, and end-user profiles. Web-based interfaces can also be made available to every business unit. IT/Operations is integrated with the Event Correlation Service, a rules-based event management service.

The HP OpenView IT Service Manager Modules

Service Level Manager provide the means to define services, stipulate their required availability and determine their supporting elements, and gauge whether service level agreements have been met. When service response times are exceeded, IT specialists can notify management and/or escalate the problem, and users can be kept abreast of the progress of outstanding issues.

Configuration Manager is used to record configuration items and infrastructural relationships. Configuration items such as hardware, software, network components and documentation can be registered and maintained, categorized and structured. An optional barcode module can be used to facilitate configuration audits. IT infrastructure data stored in Configuration Manager can be accessed from all other HP OpenView IT Service Manager modules.

Helpdesk Manager is designed to register service calls and/or support requests. A call is tracked and solved in a procedural manner by entering the service call, tracking the configuration item to which it applies, recording the name of the caller and dispatching the call to an IT specialist. This process is largely automated via integration with Configuration Manager and Service Level Manager. When a call cannot be completely resolved, Problem Manager analyzes the underlying problem and identifies its root cause.

Change Manager supports Requests For Change (RFC), impact assessments, and authorization, enabling implementation and evaluation of changes within the IT infrastructure. Change Manager tracks a change from the moment it is proposed until the change is implemented in the live environment. Before a request is approved, a risk and impact analysis is performed, in which the specific areas influenced by the change are

identified. For changes that are made frequently, a standard change set can be created.
Software Control and Distribution (SC&D) Manager controls the software life cycle from development to distribution and implementation. Software control is enforced by registering software items in the Configuration Manager Database (CMDB). SC&D Manager controls and authorizes software activities such as storing and extracting software. Software distribution controls releases of applications or updates as software items from the CMDB and manages distribution lists that define the deployment of releases. SC&D Manager is integrated with Configuration Manager and Change Manager and its processes can be automated with the use of additional tools.
Cost Manager allows costs associated with Service Level Agreements to be checked to ensure target objectives are met.
Report Manager creates reports that are directly linked to the processes within IT Service Manager.

Microsoft SMS

Microsoft Systems Management Server (SMS), although it lacks the ability to manage real heterogeneous environments that have Unix, OS/400 or even Novell NetWare, it is very capable of managing the MS Windows desktop environment called for by Commonwealth guidelines.

SMS's capabilities include print, file services and management, user administration, security, automated asset inventory, and software distribution for MS Windows 3.x, 95, NT, IBM OS/2, and Macintosh OS desktops. However it does not provide customer help desk solutions for trouble ticketing and service management.

One nice feature from the systems administrator viewpoint, is the remote console capability. This capability enables administrators to view and take actions at the user's desktop, when allowed to by the user, and to assist in them in resolving problems.

The major vendors that offer integrated solutions (CA Unicenter TNG and IBM/Tivoli TME 10) also provide capabilities for integrating with SMS. Thus, SMS offers a scalable solution for systems management of small agency Microsoft environments, with the ability to be integrated, if necessary, with the more powerful integrated solutions on the market.

Therefore, the Commonwealth and its agencies should consider investing in Microsoft SMS as a desktop management solution for Microsoft environments. However, it does not provide an integrated management solution.

Novell NMS

Novell's NetWare Management System (NMS), is a DOS/Windows-based open management platform for managing NetWare environments-both the Novell pieces of the network, and other network elements as well. Because of the large market share that Novell enjoys, many application developers have been attracted to NMS. It is more like HP's DOS version of OpenView than any of the other platforms discussed here and is not suitable as the basis for an enterprise management system. The principal problem with NMS is that it is not aimed at providing the robustness or abstraction required for an enterprise management environment.

Since the Commonwealth is moving toward a Microsoft based desktop and server environment, the Commonwealth and its agencies should altogether avoid investing in Novell NMS as either LAN or enterprise management solution.

Network Elements and Management Responsibilities

Managed Network Elements

The Commonwealth's management system must be capable of monitoring and modifying management information for the following elements (building blocks):

LAN hubs, bridges, and routers (core hubs and group hubs)
UNIX, Windows 3.x, 95, and NT end systems and servers
public networks and backbone transmission services

Each of these components will be managed by either ITD CSB or by individual agencies. Management of each of these devices and assignment of management responsibility are described in this section of the guideline document.

Foundation for Network Management: Intelligent Hubs

A management system is only as good as the raw data it collects. The management service can't manage devices for which there is no management data available. **The key strategy for universal management instrumentation within the Commonwealth enterprise network is the core hub**. By basing the physical network architecture on the hub, a diverse set of LANs, campus networks, and WANs can be managed in an integrated and increasingly automated fashion. **Management via the core hub will continue to be supplemented through existing modem and DSU management applications where appropriate**.

Hubs provide a management framework for internet components that is partially implemented in hardware. When a hub module is plugged into the hub enclosure, its presence is automatically relayed to a management system along with information on the module's identity and configuration. This allows for automatic tracking of internet configuration (largely solving the configuration management problem). Hub concentrator modules also automatically track information on the devices plugged into them, relaying to the management system the MAC and IP addresses of devices cross-referenced with their physical port number and hub number. This is invaluable information for troubleshooting purposes.

Hubs contain standardized management modules that can report to a hub management station or to another management system. Whether the management system will interact directly with a hub or through a hub management station will depend on the particular hubs chosen by ITD for the Core Hubs, and by agencies for the Group Hubs.

Management of Core Hubs and Group Hubs - a responsibility of ITD CSB and each Agency

As indicated in Figure 8 (same as Figure 1), agencies interface to MAGNET at the "Service Access Point" (SAP). The SAPs indicate the line of demarcation between components of the network managed by ITD CSB and the components managed by individual agencies. For convenience, components on the MAGNET side of the SAP are identified as "Core Hubs" (CH), and those components on the agency side of the SAP are identified as "Group Hubs" (GH).

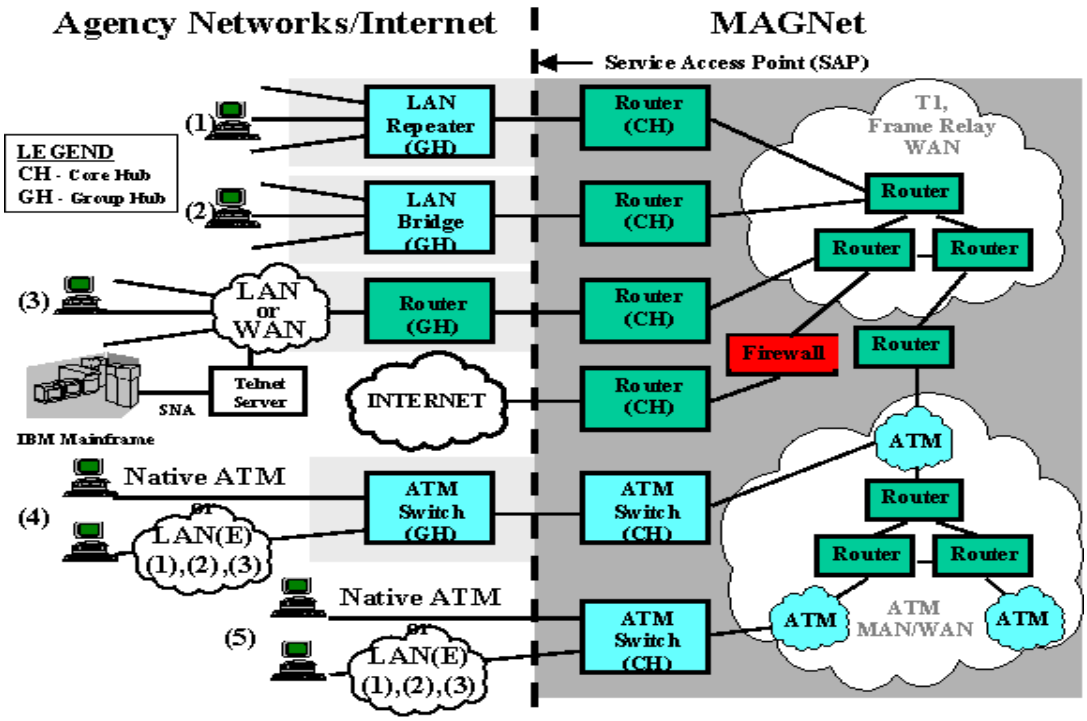

Figure 8: Separation of Management Domains

The management of the logical network is shared between individual state agencies and the Information Technology Division's Communications Service Bureau (ITD CSB). Agencies have the responsibility of managing the logical network from the end-systems to and including the GH, while ITD CSB manages the logical network from and including the CH into the wide-area. The links between the GH and the CH may fall into a shared management domain, but is usually the responsibility of the agency. Large executive agencies with internetworking expertise may negotiate with ITD CSB to manage this link, or at their discretion, request that this link be managed for them. It is, however, in the best interest of individual agencies to have ITD CSB manage the GH-CH links wherever possible. The GH-CH connections are stable and will not change as frequently as the GH-ES links. Agencies operating with limited resources probably do not have the personnel or the training dollars to take on this responsibility.

Figure 8 illustrates the separation in logical network responsibilities. Components to the right of the SAP are normally managed by ITD CSB, and those to the left of the SAP are normally managed by the agencies. Agencies may negotiate with ITD CSB to manage the GHs.

ITD CSB establishes the guidelines for the protocols that may traverse between CHs in the MAGNet backbones while individual agencies have the freedom to

choose the logical networks they will support and use. For those protocols which will be used on an enterprise scale, ITD CSB has the responsibility for naming and address policy/distribution. ITD CSB has acquired two Class-B IP address for the Commonwealth and all of its agencies. ITD CSB has the responsibility for providing blocks of addresses to individual state agencies, which in turn have the responsibility for assigning addresses to particular network devices.

Shared management of the GH-CH link will be easiest to achieve where agencies deploy the Commonwealth's standard management applications and platform. Consistent implementation decisions will allow agency and ITD CSB staff to leverage each other's expertise and capabilities. Further, implementing the same platform for managing both the backbone and agency networks will provide agencies a window into to monitor traffic and activity levels between that agency's many sites.

Although it is strongly recommended that agencies implement the same network management system to manage their local networks that is used to manage the core hubs within the backbone, this will not always be possible. However, such agencies must still deploy network management solutions that comply with the major network architectural requirements set forth in this document. The most important of these requirements for network management is for an open manager-agent communications mechanism using the SNMP protocol.

Management of Servers and End Systems - a responsibility of each Agency

The one piece of advice that was universally given for systems management in the past was: **wherever possible, reduce the systems management problem to a server management problem**. To whatever degree possible, try to eliminate the need to manage individual client systems. The strategy was to have clients load much of their software from common servers from which all software configuration and installation was done. In effect this is what is known as the "thin client" strategy. The assumption was that there are far fewer servers than clients, and the reliability of access to servers is far greater. Users often turn their client desktops off when they go home, but servers will stay on, available to receive software and configuration updates. This strategy was expected to provide an effective way to reduce the need to manage large numbers of desktops.

While the above advice is still sound, the reality is that the Commonwealth has adopted a "fat client" strategy, where desktop computers maintain their own full complement of software. In such an environment, it is desirable to instrument each client with a basic management agent. One should note, however, that the servers often still serve as the focal point for managing software distribution and uploading desktop inventory information.

Products now exist that make software distribution to the desktop relatively easy, including distribution of new versions of the operating system, updates to applications, and new configuration files. In addition, these products provide the additional advantage of automated hardware and software inventory, remote problem diagnosis, and performance monitoring.

Servers are proliferating in the environment, especially now that most desktops can also become servers. The requirements for server management include those for desktop management, e.g., software distribution, inventory, and remote diagnosis. In addition, servers need capabilities for user administration, real time status and performance monitoring and notification, and workload management. The same systems management products used for desktop management also include the server management capabilities.

A major change in systems management products is that they have capabilities for policy based management. This enables the definitions of management domains, the policies that apply to those domains, and mechanisms to enforce those policies. Another change is the ability to operate on collections of resources with a single operation. This is effectively a "force multiplier" that enables a single administrator to consistently manage tens of servers and hundreds, or even thousands, of client systems.

Operators can with a "single click" perform operations on collections of resources when doing software distribution, automated hardware and software inventory, remote problem diagnosis, user administration, real time status and performance monitoring and notification, and workload management. These capabilities for policy based management can significantly reduce the total cost of ownership to the Commonwealth and improve the quality of service to end-users.

Another change occurring is the trend toward distributed component based applications (e.g., Peoplesoft, SAP R/3) that communicate over the network using application layer "middleware", e.g., CORBA- or DCOM-based or message queuing based (Cross-Bridge based on IBM MQSeries). The staff capable of managing these component based applications and middleware are scarce. In addition, the component based applications and middleware may cross agency boundaries and require shared data repositories. Opportunities exist to achieve economies of scale and minimizing the requirement for scarce staff by centralizing some management responsibilities.

We recommend that the Commonwealth and agencies evaluate current systems management products for appropriate use within their environment. We also recommend that the Commonwealth investigate the opportunities for centralizing within ITD some of the systems and application management responsibilities currently performed by individual agencies so as to reduce the need for scarce skilled staff and achieve economies of scale. Candidates for centralization include, but are not

limited to: system backups, software distribution, inventory, and system and applications monitoring.

Management of Public Networks and Backbone Transmission Services - a responsibility of ITD CSB

Public network services (analog leased lines, DDS, and T-1) from the telephone service provider provide the raw bandwidth needed to operate the backbone. **To ensure that the telephone service provider is providing adequate service levels and responding to outages in a timely manner, management of these resources must be concentrated within ITD CSB. Additionally, ITD should work with the telephone service provider to provide a management window into the public network**. This window may be implemented via a management system gateway into the telephone service provider environment, or through a dedicated console provided to the Commonwealth by the telephone service provider. While individual agencies may wish to monitor the logical configuration of the Commonwealth's internet to ensure that ITD provides reasonable service to them, ITD CSB will want to monitor the telephone service provider to ensure that they are providing the State with the required bandwidth at reasonable service levels.

Management Recommendations

The major goal of developing an enterprise management architecture is improved manageability. This translates into higher productivity for support staff, lower network costs and, most importantly, greater responsiveness to user needs. To achieve improvements in manageability will require the Commonwealth and its agencies to change their approach to management on many fronts. The Commonwealth should undertake the following initiatives to implement an effective and efficient end-to-end systems, applications, and network management solution.

Adopt a "Build-Forward" Approach

The Commonwealth should adopt a build-forward approach to procuring and implementing an enterprise management strategy. A build-forward strategy means that all new computing and communications assets, whether servers, desktops, or LANs, must conform to a set of management standards that will allow such assets to be integrated into the enterprise network management environment. A build-forward approach to managing the network allows existing legacy devices to continue to be managed via whatever management applications are currently in place. This approach preserves the investment the Commonwealth and its agencies have already made in legacy management systems. However, further investment in better management of legacy networking devices is not warranted. A principal rationale for adopting a build-

forward strategy is that the Commonwealth has committed to deploy major new applications and systems using distributed computing and internetworking technology wherever possible. This strategy seeks to eliminate the Commonwealth's dependency on legacy systems, making legacy management increasingly less valuable.

Although the Commonwealth will deploy new management applications for newly acquired networks and systems, several key element management systems will remain in widespread use for the next several years. These element management systems include the:

AT&T Paradyne Network Management System
Teleglobe Modem Management System
NetView for management of the mainframe as a host system
Unisys management environment for Unisys agency systems
(Megaview) T-1 multiplexer management system

In addition to these legacy management applications, various agencies may be using other applications to manage particular networks and systems. However, as new systems are deployed, or old systems decommissioned, all agency and networking elements should be managed via the State's open management platform standards for network and systems management.

Adopt an Integrated Management Architecture

We recommend that the agencies within the Commonwealth adopt an architecture that is consistent with an integrated systems, applications, and network management approach based on an open management platform. The details of such an architecture should be appropriate to the environment to be managed:

Integrated Systems, Applications, and Network Management

The Commonwealth should investigate whether environments exist within agencies that are of sufficient scale in numbers and heterogeneity of managed servers, desktops, and networking components as to potentially warrant an integrated approach to their management. It should keep in mind that although the potential payback is high in terms of reduced costs and improved quality of service, past indications are that the risk of failure is about 70%. Special emphasis should be given to assessing the impact on the IT organizations, their current processes, and staff skills that such an integrated approach may require.

If the Commonwealth determines that environments exist for which an integrated systems, applications, and network management approach is appropriate, then they should evaluate and select one of the leading vendors of such product suites as the standard for the Commonwealth.

Network Management

MAGNet and Agency networks containing SNMP manageable devices - The Commonwealth has selected for management of MAGNet a robust open management platform that provides SNMP management capabilities. **Agencies with networks that contain SNMP manageable devices should consider adopting the same OMP product, or products from the same family which are scaled to meet their requirements. We further recommend that the Commonwealth select the latest version of SNMP wherever interoperability between managers and agents can be assured.**

Agency LANs containing no SNMP manageable devices - in those instances where the agency has no manageable LAN components, e.g., the agency devices connect directly to ports on the group hub which is managed by ITD CSB, no device management is required by the agency - hence no network manager is required.

Legacy non-SNMP network devices - legacy network devices that are not SNMP compatible should be phased out and replaced by SNMP compatible devices. In those cases where phase out is not reasonable, consideration should be given to development of an SNMP proxy that is capable of communicating to the legacy devices in their native management language, translating native commands into SNMP, and communicating via SNMP with an SNMP capable manager.

Systems and Applications Management

Mixed Unix and NT server/workstation environment - We recommend that the Commonwealth select a robust open management platform that can manage this mixed systems environment - in particular with respect to hardware and software inventory management, software distribution, user administration, and application and database monitoring. Furthermore, we recommend that the selected platform should integrate with the chosen integrated systems, application, and network management solution.

Desktop environment - The Commonwealth has decided to standardize on Windows NT Server Version 4.0 (or greater) for new servers, and Windows NT workstations. Existing Banyan and Novell networks, if retained, must be migrated to the version levels that interwork over TCP/IP. **We recommend that the Commonwealth select a robust open management platform that can manage the new standard desktop environment - in particular with respect to hardware and software inventory management, software distribution, user administration, and application and database monitoring. Consideration should be given to the platform's ability to manage the existing Novell and Banyan environment. In addition, the platform should be scalable such that it is cost effective for managing the different sized**

agency environments found in the Commonwealth. Furthermore, we recommend that the selected platform should integrate with the integrated systems, application, and network management solution - should one be selected.

Standardize on SNMP for Network Management

The Simple Network Management Protocol (SNMP), is a widely used protocol in the network management arena. It is by far the leading standard for network management. The latest fielded version of SNMP (known as SNMPv2) adds important new capabilities to the protocol. It makes SNMP a more robust management protocol by offering better efficiency, error control, and manager-manager communications. The latest version of SNMP (SNMPv3) has just been approved as a draft Internet standard. It adds the security that has been greatly needed in enterprise management environments. **We recommend that the Commonwealth select a robust open management platform for network management that provides robust SNMP management capabilities. SNMP management will be the foundation of network management for MAGNET internal devices, core hubs, group hubs, and agency networks. We further recommend that the Commonwealth select network devices having the latest version of SNMP, and upgrade existing devices to the latest SNMP version, wherever possible and interoperability between managers and agents can be assured. Similarly, manager workstations should be selected or upgraded to support all SNMP versions necessary to support the network devices.**

SNMP will be used to collect alarms and to monitor the availability of network elements. SNMPv3 will provide authenticated exchanges between manager and agent so that unauthorized machines may not masquerade as a management system. This capability will enable the use of SNMP for configuration and control functions. Statistics on usage and performance will also be collected using SNMP. There is a large and growing body of standard MIB definitions (standard libraries of management functions that can be performed on network elements such as bridges and routers) based on the SNMP MIB structure, and these will provide a good basis for initial efforts at proactive problem resolution.

It is our recommendation that the Commonwealth not standardize on the Common Management Information Protocol (CMIP), which is the OSI standard for network and systems management. CMIP standard defines a more complex and fully featured protocol and MIB structure, but has not received widespread acceptance in the Internet marketplace. Therefore, its has fewer implementations and is relatively more expensive than SNMP management. However, CMIP may be used in special cases where particular network elements require functionality which management via CMIP can provide. Management of such devices will still be possible via an open (SNMP) management platform

since most platforms (with the exception of SunNet Manager) now support both SNMP and CMIP.

Standardize on a Common Platform for Network Management

ITD has chosen a management platform for MAGNET, with compatible management applications appropriate to the management of MAGNET network devices. Acquisition, support, and training economies could result from agencies standardizing on the same network management platform used by ITD. In addition, such standardization would allow treatment of the ITD and agency managers as one distributed management platform with the potential for data sharing and flexible partitioning of management responsibilities between ITD and the agencies. This would allow for reducing the need for scarce skilled networking staff. **It is strongly recommended that agencies implement the same network management platform as ITD, or platforms from the same product family that are scaled to meet their requirements."**

Standardize on Standard Object-Oriented Frameworks for Systems Management

Systems management requirements are significantly different from those for network management. Accordingly, the framework and protocols suitable for network management are inadequate to provide fully the required systems management functionality.

The object-oriented paradigm has become accepted within the systems and applications management community. The two accepted implementation architectures are the Common Object Request Broker Architecture (CORBA) standard, and Microsoft's Distributed Common Object Model Architecture, a defacto standard. Both use a remote procedure call (RPC) protocol for exchanging messages.

We recommend that the Commonwealth and its agencies adopt systems management products that are founded on the CORBA and DCOM object models.

Provide Major Management Applications

An integrated systems and network management solution provides a single enterprise-wide view of the network to operations staff via a standardized user interface. The deployment of an open management platform should, at a minimum, provide a basic real-time monitoring capability focused on alarms. However, other key applications are needed to improve the effectiveness and coordination of the key management work processes in network and distributed systems management. These key applications include:

a workflow management system that includes capabilities for:
problem management (trouble ticket system)
change management that is comprised of at least two major parts: a change notification system and a work order scheduling system
escalation procedures for unresolved problem and service requests
an inventory management system
a network measurement and capacity planning system that is also comprised of multiple parts, including: traffic monitoring, baselining, and modeling tools.

In order to provide an integrated management solution, the Commonwealth must select network and systems management platforms that are capable of providing applications in each of these areas. Although different applications will be used to handle Accounting and Performance management, these applications must be able to reside and operate on the same management platform. Applications for Fault, Configuration, Security and Accounting management are the most critical to acquire first.

Most applications will be focused on automating routine administrative tasks (problem management, inventory management, change management, and accounting) performed by ITD CSB and individual agencies. While these applications will be initially deployed for either agency-only or ITD-only use, many of them (ideally) will evolve into groupware applications that enable distributed work teams to coordinate their actions. This will make network troubleshooting, equipment installation, and proactive management significantly easier. Some management applications add efficiency to the management process by allowing end users to report problems and to request changes electronically.

Identify, Document Management Processes and Train Staff

All of the tools available for network and distributed systems management will be useless if the processes are not in place to make effective use of the tools, and the staff are not trained in their use.

We recommend that the Commonwealth and the agencies perform an assessment of their management processes and procedures before acquiring new management tools, and properly document and adapt those processes and procedures to make the tools most effective.

We recommend that the Commonwealth provide proper training for the staff that are expected to make use of the management tools - both in the tool capabilities, and in the proper application of those capabilities to effect the procedures and processes required to effect management actions.

Conclusion

Together, these applications and standards satisfy the five major requirements of network management systems:

- Fault Management
- Configuration and Name Management
- Performance Management
- Security Management
- Accounting Management

These applications and standards will provide the biggest increase in management efficiency and effectiveness when they are standardized across many of the Commonwealth's agencies.